Lawrence Livermore National Laboratory

The INFOSEC Research Council (IRC)

and the

National INFOSEC Technical Baselines (NITB)

April 29, 1997

Doug Mansur, Program Manager
Computer Security Technology Center

UCRL-MI-127596

Outline

- **INFOSEC Research Council**
  - **Purpose**
  - **Members**
- **National INFOSEC Technical Baselines**
  - **Intrusion Detection**
  - **Firewalls**

INFOSEC Research Council

- The IRC is intended to promote intelligent research investments with limited resources
- Achieve a force multiplication effect in addressing the complex set of national INFOSEC problems
- The IRC includes U.S. Government sponsors of information security research from the DoD, Intelligence Community, and other Federal Agencies

Current IRC Members

- Naval Research Laboratory (NRL)
- Space and Naval Warfare Center (SPAWAR)
- Office of Naval Research (ONR)
- Air Force Information Warfare Center (AFIWC)
- Air Force Rome Laboratory (RL)
- U.S. Army Communications-Electronics Command (CECOM)
- National Security Agency (NSA)
- National Institute of Standards and Technology (NIST)
- Department of Energy (DOE)
- Central Intelligence Agency (CIA)
- Defense Information Systems Agency (DISA)
- U.S. Army Land Information Warfare Activity (LIWA)
- Defense Advanced Research Projects Agency (DARPA)

INFOSEC Research Council (Cont.)

- The council provides a community-wide forum to:
  - Discuss critical INFOSEC issues
  - Convey the research needs of their respective communities
  - Describe current research initiatives and proposed courses of action for future research investments
- By participating in the IRC, sponsors can:
  - Obtain and share valuable information that will help focus their INFOSEC research programs
  - Identify high-leverage, high-level research targets of opportunity
  - Minimize duplication of research

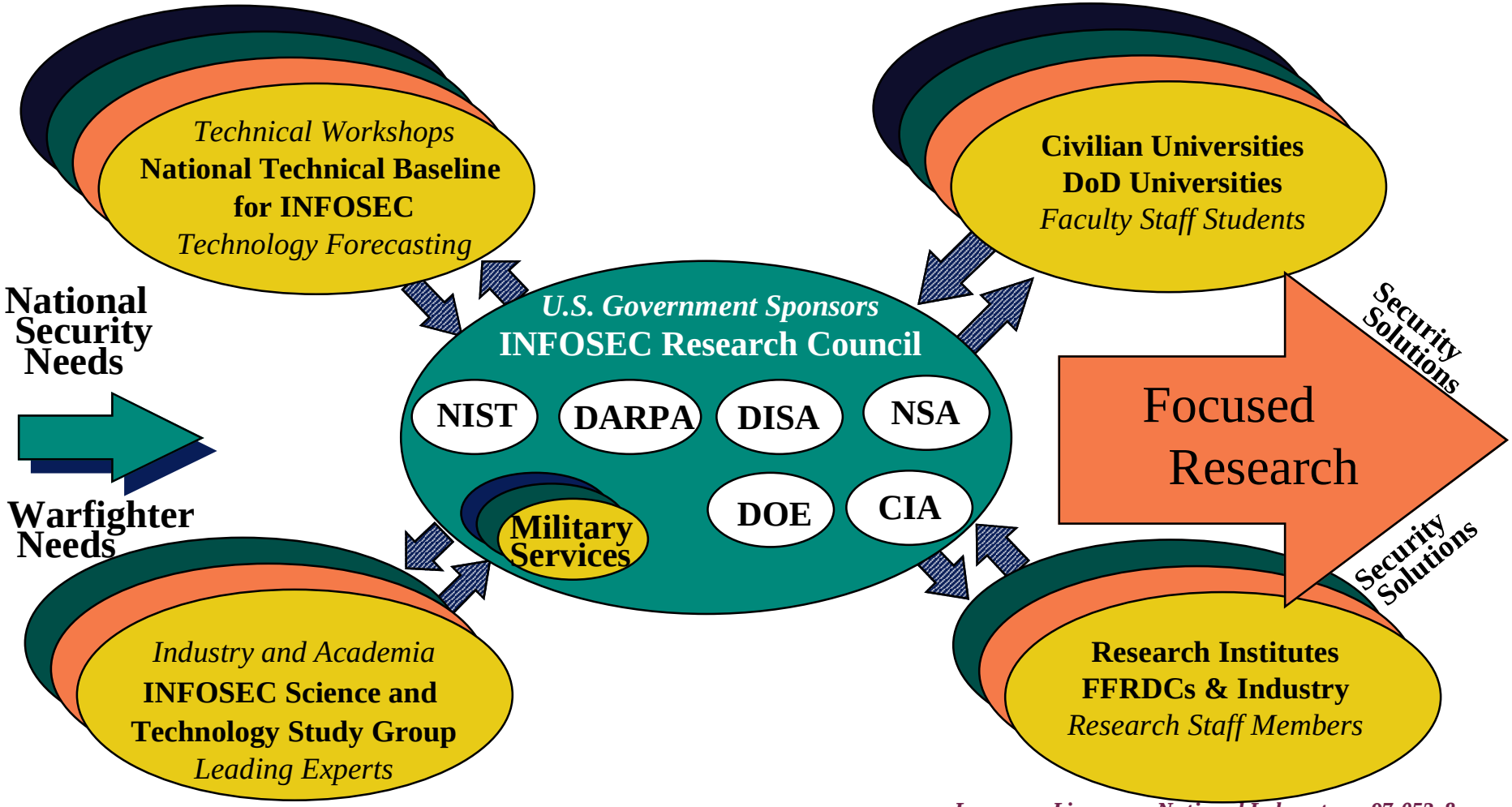
INFOSEC Research Council (Cont.)

- The National Technical Baseline establishes the current state of the practice for information system security
- Partnership between NSA and the DOE National Laboratories to:
  - Bring together the collective national wisdom in a particular INFOSEC science or technology area
  - Collect and consolidate all relevant information in that area
  - Establish and maintain a baseline on current knowledge in that science or technology area

INFOSEC Research Council (Cont.)

- Data collection through a variety of venues:
  - Meeting with leading experts
  - Leveraging off workshops conducted by others
  - Literature review

National INFOSEC Technology Baseline



Outline


Purpose/Audience
Current Studies
- Intrusion Detection
- Firewalls
Future Studies

What is a National INFOSEC Technology Baseline

- Provides state-of-the-national technical capability for critical INFOSEC areas
- Focus the attention of research community or the most difficult and challenging areas (gaps)
- Identify promising future R&D approaches
- Provide input to the process for prioritizing future R&D efforts

Target Audience

- INFOSEC Research Council (IRC)
- Researchers
- Computer security practitioners
- Vendor community

Two completed studies . . .

- NITB #1: *National INFOSEC Technical Baseline–Intrusion Detection and Response*, October 1996, PI: Dr. Fred Cohen/SNLA, url:http://doe-is.llnl.gov/nitb/ids.html*
- NITB #2: *National INFOSEC Technical Baseline–Firewalls* (draft), April 1997, PI: Steve Cooper/LLNL, url:http://doe-is.llnl.gov/nitb/firewalls.html (available approximately May 19)

*Contains the papers on-line references, pointers to other interesting sites, info on existing systems, etc.

National INFOSEC Technical Baseline

Intrusion Detection and Response

by

Lawrence Livermore National Laboratory
Sandia National Laboratories

(and many others)

Intrusion Detection and Response

- Scope of this study
  - Intrusion detection and response is very big
    - » Motion sensors to real-time fraud detection
  - Our scope somewhat more limited
    - » Non-physical intrusions (bits)
    - » Digital electronic components of the GII
      - End user nodes (phones/computers/set-top-boxes)
      - Networks (cable/satellite/LANs/phones . . .)
      - Control systems (DNS/phone switches . . .)
      - Infrastructure (power/ air conditioners . . .)
    - » Below the application level

Background on ID

- Detection and response come from attacks
  - Application level against financial systems
  - Against phone systems in 1950s on
  - Then against network infrastructures
  - Eventually against hosts
- Reactively created field
  - Response to market need
  - Historically chases attackers

Major Findings

- Issues of time
  - Harm increasing and rate increasing
  - Time to attack decreasing (automation)
  - Some systems require 1ms response
  - Reflexive control issues (self-denial of services)

Major Findings (Cont.)

- Issues of definition
  - What is an intrusion:
    - » Differing views:
      - > by different communities
      - > in different countries
      - > within the research community
    - » Examples
      - “safe” ==>> “unsafe” state
      - any “unauthorized” activity
      - activity that violates site policy
      - any action resulting in corruption, leakage, denial

Legal Views

- IDSs are viewed by some as intrusive
  - privacy rights/worker monitoring
- Some legal staff assert unattainable goals
  - <0.01% false positive rates or can’t use
- Others claim unlimited use OK
  - policy the company owns it all
- Authoritive judgments not yet made
- Many complex issues

Major Findings

- In general:
  - Useful tools are available today
  - Highly trained users required
  - Must be customized for a given environment

Specifically, current systems:

- Reliably detect a substantial number at known intrusion techniques
- Detect substantial short-term changes in user or system behavior
- Produce many alarms that, on investigation, are not intrusions (false-positives)
- Fails to alarm on an unknown number of intrusions (false-negatives)
- Also, as a commercial industry becoming healthy and competitive, for example, Haystack Labs, The Wheel Group, etc.

What is needed

- More sharing of signatures/cooperation
- Better testing (Mitre, Lincoln Labs, others)
- Context boundedness: audit trails lack data, can't tell if protection by-passed
- Scaling to really large networks?
- Little fundamental theory
- Need: more work in automated recovery/response
- Some new tricks
  - calling patterns, traffic analysis
  - calling instrument electrical characteristics
  - "policy based" monitoring

National INFOSEC Technical Baseline

Firewalls

by

Lawrence Livermore National Laboratory

Sandia National Laboratories

(and many others)

The report outline

- Executive Summary
- Introduction
- Background (justification, history)
- Theory of Operation
- The Marketplace
- Findings
- *Appendix A: Commercial Features & Technologies (proposed)*
- Bibliography (57 references)

The Firewall, defined

- The firewall is a collection of components placed between two (or more) networks such that:
  - All traffic from inside to outside, and vice-versa, must pass through the firewall
  - Only authorized traffic, as defined by the security policy, will pass through the firewall
  - The firewall itself is immune to penetration

Why a firewall?

- As protection against the Internet
- For creating security domains
- For enforcing security policy

Where did firewalls come from?

- Multilevel systems and security models received a lot of research attention in the ‘70s and ‘80s
- Firewalls seem to have followed their own evolution, starting in the ‘80s?
  - Pacific Bell
  - AT&T
  - Digital Equipment

Firewall Evolution

- Screening routers
- Gateways
- TCP Wrappers
- Gates & Chokes
- Firewall Toolkit
- Commercial Firewalls
- Recognition of Firewalls

Physical Components

- Packet filters
  - Visible
  - Invisible
- Application proxies and circuit gateways
- Bastion hosts

Firewall Features

- Authentication
- Encryption
- Auditing

Firewall Limitations

- Physical Limitations
  - A firewall doesn't protect against malicious insiders
  - A firewall doesn't offer protection for connections that don't go through it
  - Firewalls are never completely transparent, introducing transit delays, bottlenecks, and single point-of-failure
- Others
  - A firewall can't protect against completely new threats
  - A firewall is only a perimeter defense; users may require end-to-end security
  - A firewall is limited against content-based attacks

Changing Paradigms

- New networking technologies
  - ATM
  - Switched LANs
- New protocols
  - IPv6
- The World Wide Web
  - Changing the applications base and the way people use networks

The Firewall Marketplace

- Rapid growth for commercial firewalls
  - Approximately 60 products
  - Many more vendors of consulting, other firewall services
- Product evaluation and certification services
  - But how valid is firewall validation?
- Free stuff
  - socks libraries
  - TCP Wrappers
  - TIS Firewall Toolkit
- Firewall Savvy Applications

Conclusions

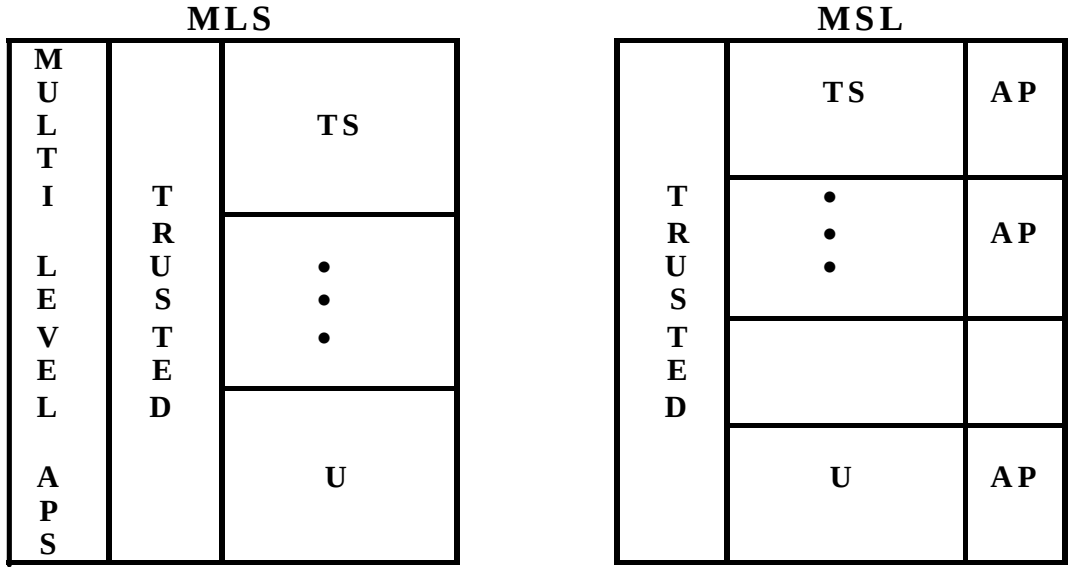
- Firewalls are a mature technology
- They have their limitations
- What is needed is a better capability to integrate them into a larger security context
  - User interfaces and management
  - Interoperability
  - Standardization

Future studies . . .

- NITB #3: *Multilevel Secure (MLS) and Multiple Security Level (MSL) Systems*
  - What is available today?
  - How are these systems used in real environments?
  - What are their major strengths and weaknesses?
  - Future directions for R&D?
  - If time permits: V&V, assurance, mechanisms

Multilevel Secure (MLS) vs Multiple Security Level (MSL)

- MLS: ". . . trusted to properly maintain and keep separate data of different security levels, categories, or compartments." [1]
- MSL: Isolates levels, etc., but not direct sharing between levels.



[1] National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, June 5, 1992.

Future studies . . .

NITB #4: *Network and Host Security Administration*

- Major goals:
  - What is the capability for secure administration of networks and collections of hosts?
  - What tools are available? (network-wide basis)
  - For: larger networks
  - Look at existing experience of large networks
    - » (AT&T, MCI, Sprint, IBM, DISA)
  - Also look at SCADA system examples
  - Report on problems in securely managing networks

Future studies . . . , (Cont.)

- Minor goals
  - Briefly discuss other general security tools
    - » COPS
    - » SPI-NET
    - » Icepick
    - » SATAN
    - » ISS
    - » etc.
  - Defer to future study: PKI, DCE, Kerberos, CORBA, DCOM, etc.

Request for assistance . . .

- Interested in doing a study? (some funding available)
- We need:
  - Names of key experts
  - Professional-quality articles
  - Lists of products and their features
  - Bibliographies
  - Useful Web sites, etc.

- Contact info:

  Doug Mansur (mansur@llnl.gov)

  (510) 422-0896

  http://doe-is.llnl.gov/nitb